MICROSOFT WINDOWS® 2000

CONSIDERATIONS FOR DOD IT Organizations

Mr. Steve Stefanini
COE Engineering Office
stefanis@ncr.disa.mil

Ron Robertson
Lowell Rosen
The MITRE Corporation
thor@mitre.org
lrosen@mitre.org

March 2000

EXECUTIVE SUMMARY

Microsoft Corporation announced in December 1999 that they released to manufacturing their latest operating system, Windows® 2000. Computer manufacturers like Dell, Compaq and IBM have been working closely with Microsoft during the development stages and are offering free upgrades to customers with pre-installed versions of Windows® NT. A commercial release of Windows® 2000 Professional, Windows® 2000 Server, and Windows® 2000 Advanced Server was scheduled for February 17, 2000. The DII COE Engineering Office is closely monitoring Windows® 2000 activities in the corporate, academic, and research communities, and working with interested U.S. Agencies and Services.

Windows® 2000 is more than just the next release of Microsoft's Windows® NT operating system. It has taken Microsoft Corporation over four years, working closely with many partners, to engineer, integrate, test, and refine this next generation operating system. Although the user interface is similar to Windows® 98, the underlying operating system architecture and services have been significantly enhanced and augmented. Windows 2000® is "feature-rich" including several new and enhanced features: directory services, network services and protocols, and security, robustness, and scalability. Of these many enhancements, the single most significant component of Windows® 2000 is the integrated, hierarchical, distributed, and replicated directory services – the Active Directory.

Directory Services have been used in the computer industry for years, with many vendors providing directory solutions. Windows® 2000 uses an X.500-based directory service called the Active Directory for the storage of key information about a Windows® 2000 environment. The directory supports a diverse set of information including user identification, passwords, email addresses, computer names, and encryption keys. With the proliferation of X.500-based directories (e.g., DMS, Netscape Directory Service, Sun Microsystems' Directory Service), it is has become paramount that Information Technology (IT) organizations begin to plan for the coexistence or integration of these directories.

Windows® 2000 also includes a diverse set of standard security features that are available programmatically through the Security Support Provider Interface. A major security component is the integrated Kerberos network authentication protocol providing strong authentication through applied secret-key cryptography. To complement standard user authentication, additional security services include the Encrypting File System, Public-Key Infrastructure, Smart Card, Internet Protocol Security (IPSec), and Virtual Private Network (VPN).

Windows® 2000 networking has significantly changed. New and enhanced network services include: TCP/IP as the new default network protocol for all versions of Windows® 2000; optional network packet encryption; quality of service and bandwidth allocation and management; support for the resource ReSerVation Protocol (RSVP); support for Multicast Internet protocols (MBONE); support for IEEE 802.1p prioritized LANs, and virtual private networks.

Windows® 2000 Advanced Server and DataCenter Server versions include the most complete set of features of the Windows® 2000 operating system: high availability, and the kind of scalability required for enterprise and large departmental solutions. Key scalability and robustness features include Network Load Balancing (NLB), the Microsoft Cluster Service, and symmetric multiprocessing (SMP).

Treating Windows® 2000 as a mere upgrade to an installed base of Windows® NT workstations and servers is an almost sure path to operational difficulties and significant rework. Microsoft and a wide variety of industry consulting firms agree: there are a number of factors to consider, tradeoff decisions to reach, tests and evaluations to perform, and step-by-step transition strategies to decide in order to accomplish a successful migration.

For IT organizations that are primarily Windows® NT-based, Windows® 2000 is very attractive and compelling. However, DOD systems tend to be *heterogeneous*, meaning that computers from different vendors, with different operating systems, must work together in a coordinated network. In this type of environment, the following principles can help ensure a successful migration:

Don't Be An Early Adopter. Since Microsoft plans to support Windows® NT for at least a few more years, you don't necessarily have to deploy Windows® 2000 right away. You have the time to plan your migration/conversion carefully. **Be An Early Tester** of the technologies and services in a prototypical environment as an aid in determining how well they interoperate with your legacy systems. **Develop Guidelines** based on your early pilot and prototype experiences to prepare the organization for future deployment.

And, finally, remember the adage:

Plan Twice, Deploy Once

Abstract

This document provides a high-level technical discussion of the Microsoft Windows® 2000 operating system and its possible impacts on DOD Information Technology (IT) organizations. After an introduction and brief product overview, a set of technical considerations is discussed, followed by a summarization of activities an organization should undertake before deploying Windows® 2000 into an operational environment.

Keywords

DII COE, Windows® 2000, Active Directory, Domain Name System, Lightweight Directory Access Protocol, Kerberos, IPSec, VPN, Windows® NT.

Acknowledgments

Thanks go to Roger Duncan and Jesse Pirocchi of the MITRE Corporation for their timely and thoughtful editing of this paper.

TABLE OF CONTENTS

1. INTRODUCTION

The Defense Information Infrastructure (DII), in support of the warfighter, continually investigates and assesses technologies for potential inclusion into the DII Common Operating Environment (COE). This document is a technical overview of major Windows® 2000 Operating System (OS) components and features and addresses the potential impact of deploying this new OS in an operational environment. A series of technical (deployment) considerations with recommended mediation actions is presented as an aid for DOD Information Technology (IT) staff. Multiple references at the end of this document provide additional information on Windows® 2000.

Recently Microsoft Corporation, the vendor of Windows® 95, Windows® 98, and Windows® NT, announced, after four plus years of development, its latest OS, Windows® 2000. Commercial versions of Windows 2000 were expected to be available 17 February 2000, with key personal computer (PC) vendors like Dell, Compaq, and IBM providing free upgrades for systems purchased with pre-installed versions of Windows® NT. Windows® 2000 is more than "just an upgrade for Windows® NT"; it incorporates a series of new technologies and capabilities into four versions of this OS. Windows® 2000 has the potential to simplify administration and reduce total cost of ownership (TCO). However, the deployment decisions you make will have a significant impact on the benefits you realize.

There are many, diverse, documented views about Windows® 2000. Indeed, Microsoft itself has several thousands of pages (e.g., white papers, Web pages, Help). This document presents information in a "building block" model: information on the new features of Windows® 2000 is presented in Section 2; several issues that IT organizations should address before deploying Windows® 2000 are in Section 3; and summaries of conclusions and recommendations are in Section 4.

2. WINDOWS® 2000 – NEW FEATURES

Windows® 2000 capabilities are a superset of Windows® NT, incorporating powerful technology and new or enhanced features. Although Microsoft Corporation expended significant resources to develop Windows® 2000, little rigorous testing within the context of operational networks and legacy heterogeneous systems was performed. Integration and interoperation within DOD's heterogeneous environment is critical to our military missions.

In February 2000, Microsoft released three versions of Windows® 2000 (Professional, Server, Advanced Server) with an additional server version, DataCenter Server, forthcoming. Each version is targeted for a specific business/market, as reflected in Table 1. This document does not attempt to address the breadth of all new features within Windows® 2000, but rather focuses on several key components of Windows® 2000.

Windows 2000	Professional	Server	Advanced Server	DataCenter Server
Target Audiences	Business desktops, notebooks	File, print, Internet, Networking	Line of business, e-commerce	Large critical applications, OLTP, data warehouse, ASPs and ISPs
CPUs supported by 1 system	2	4	8	32
Memory	4 GB	4 GB	8 GB	64 GB
Clustering	None	None	Two-node failover, 32-node network load balancing	Cascading failover among four nodes, 32-node network load balancing
Minimum system requirements	133 MHz Pentium-compatible CPU, 64 MB RAM, 1 GB available disk space	133 MHz Pentium-compatible CPU, 128 MB RAM, 1 GB available disk space	133 MHz Pentium-compatible CPU, 256 MB RAM, 1 GB available disk space	To be announced
Estimated Price*	$319 $149 for upgrade from Windows NT Workstation 3.5.1, 4.0 $219 for upgrade from Windows 9x	$999 $499 for upgrade Includes 5 client access licenses (CALS)	$3,999 $1999 for upgrade Includes 25 client access licenses (CALS)	To be announced
Scheduled release date	17 Feb 2000	17 Feb 2000	17 Feb 2000	To be announced

* Estimated retail prices only.
Pricing and Licensing for Windows 2000 Professional (http://www.microsoft.com/windows2000/guide/professional/pricing/default.asp).
Pricing and Licensing for Windows 2000 Server (http://www.microsoft.com/windows2000/guide/server/pricing/default.asp)
Source: http://www.microsoft.com/windows2000/guide/platform/overview/default.asp

Table 1. Hardware "Footprint" and Estimated Prices

2.1 Directory Services

With the introduction of distributed computing, it has become necessary to provide mechanisms for locating diverse components scattered across the network. The resulting mechanisms provide a name resolution capability to lookup networked resources based on one or more characteristics. This capability includes, for example, Internet Protocol (IP) address and machine name, Remote Procedure Call (RPC), and Email address. Windows® 2000 has integrated the many Windows® name resolution capabilities, like the Windows® Internet Name Service (WINS), Information Locator Service (ILS), and Domain Name Server (DNS), into an integrated, hierarchical, distributed, replicated data repository.

2.1.1 Active Directory (AD)

The Active Directory is an integrated, hierarchical, distributed, and replicated directory service for managing access rights and resources across an enterprise. The Active Directory is based on Microsoft's X.500-based Exchange Directory Service, augmented with capabilities for operating system-level authentication, and resource access and control. Embedded within the Active

Directory is its schema which provides an enterprise the ability to easily enhance its definition to support unique services and features. Access control mechanisms may be attached to each object and to the properties of each object in the directory.

Functionally, the Active Directory is dependent on the Domain Name Service for locating entities or objects (e.g., Email account, user ID, machine name, printer name) within the directory. DNS provides an "entry point" for locating most directory-resident information. As seen in Figure 1, the Active Directory consolidates name resolution databases, accommodating a variety of interfaces. Conceptually, the top "layer" is an enterprise's Domain Name Service.

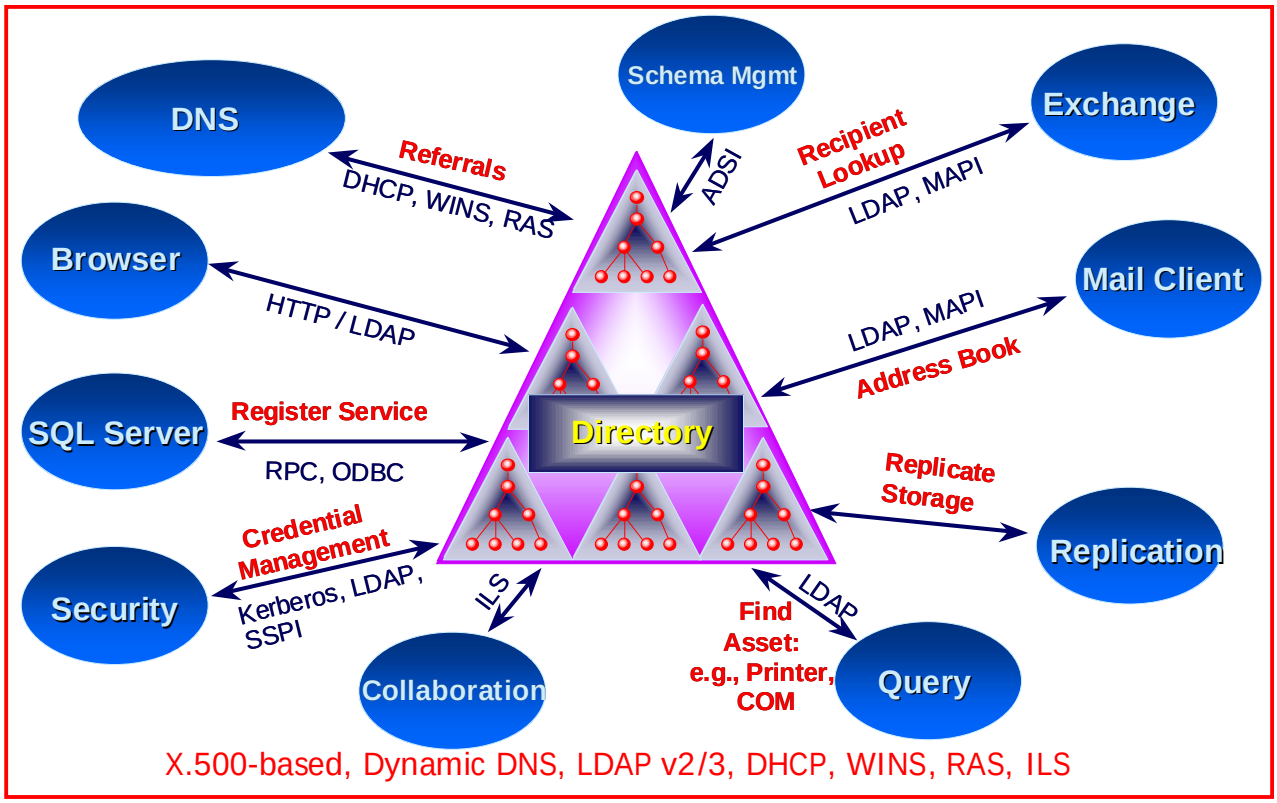

Figure 1. Windows® 2000 Active Directory Services

Due to the distributed and replicated design of the Active Directory, synchronization of this directory, within an enterprise's directory space, may be facilitated through directory design including, but not limited to: partitioning, directory and domain architectures, sites directories, and global catalogs. The inherent directory flexibility provides enterprises the opportunity to:

- extend the Active Directory's schema to support unique organizational capabilities
- partition and apply access controls based on organizational needs
- re-engineer the enterprise's collective directory services, resulting in a better, integrated directory service

The Active Directory replication model[1] is described as a multi-master database with loose consistency, and convergence. This model is used to reduce network traffic, reduce system overhead, and ensure all replicas are always in complete synchronization. When Active Directory objects or properties of an object, are added, deleted, or modified, these changes are "pushed" to all domain controllers of a Windows® 2000 domain. A series of date-time stamps and object versioning are used on each replica to aid proper synchronization among the controllers. This combination of identifiers is used to ensure the directory's data is consistent and accurate, while minimizing network and system overhead. The unit of replication is a Windows® 2000 domain. When designing the Active Directory architecture, sites play a major role in the Active Directory replication service. Site server machines differentiate between local replication (local area network) versus enterprise-level replication (wide area network).

To better support dynamic environments like roaming users, mobile users, and dial-in users, the Active Directory integrates several name resolution services, including the Dynamic Host Configuration Protocol (DHCP), Remote Access Service (RAS), Windows® Internet Name Service (WINS) and Dynamic Domain Name Service (DDNS). With this integration, as new machines are attached to the network and request an IP address via DHCP, or users dial-in through RAS, all name resolution databases are automatically updated. The Active Directory provides a level of integration never before available in a single commercial off the shelf product (COTS).

In Windows® vernacular, a **trust** is the relationship between two domains that enables pass-through authentication, in which a trusting domain honors the logon authentication of a trusted domain. Conceptually Windows® domain trusts are simple. In Windows® NT each trust is one-way, and these trusts are manually defined and managed. In Windows® 2000, trusts are two-way and transitive. For example, if domain "A" trusts domain "B", and domain "B" trusts domain "C", in a Windows® 2000 environment there is an implicit trust between domains "A" and "C", with all trusts bi-directional. Administratively and architecturally this is a significant change, with potential impacts of implied trusts between domains.

Windows® 2000 domain structures and interrelationships are an integral part of the Active Directory. An organization may select two primary approaches for migrating a Windows® NT domain environment to an Active Directory-based Windows® 2000 environment:

---

[1] "The replication model used in Microsoft® Active Directory™ is called multi-master loose consistency with convergence. In this model, the directory can have many replicas; a replication system propagates changes made at any given replica to all other replicas. The replicas are not guaranteed to be consistent with each other at any particular point in time ("loose consistency"), since changes can be applied to any replica at any time ("multi-master"). If the system is allowed to reach a steady state, in which no new updates are occurring and all previous updates have been completely replicated, all replicas are guaranteed to converge on the same set of values ("convergence")." http://msdn.microsoft.com/library/psdk/adsi/glreplic_6kdo.htm

- Domain upgrade—This approach is accomplished “in-place” on the legacy Windows® NT Primary Domain Controller and Backup Domain Controllers. Before selecting this approach, consider the major limitation: you not only inherit the outdated Windows® NT domain structure (Windows® NT domain structure, users, groups, trusts), but you also migrate possibly obsolete directory data.

- Domain restructure—This approach allows an organization to redesign the directory services based on current organizational needs, preserving most Windows® NT domain data. Organizations should realize greater benefits if they take this opportunity to carefully plan, prototype, and implement a new directory architecture.

For organizations that support multiple Internet Protocol (IP) domains, for example pentagon.mil and osd.mil, the Active Directory separates each contiguous name spaces like pentagon.mil and osd.mil into a collection of resources. Each collection is known as a “tree.” An Active Directory supporting more than one contiguous name space has multiple “trees” which are assimilated into a “forest.” This concept is important when designing a directory name space and architecture since all trees in a forest share a common schema, configuration, and global catalog.

The Active Directory architecture provides support for wide area network (WAN)-based searches. To reduce the size and local processing of a domain controller (and Active Directory replica), two additional directory concepts are important: sites, and global catalogs. A directory site server facilitates local site requests for directory information and responds to other domain access requests. The Global Catalog (GC) is a partial replica, consisting of a minimal set of directory information necessary to aid in distributed directory searches .

From an end-user's perspective, the Active Directory provides a capability to search across the enterprise. For example, a user could query the directory for the names and location of all color laser printers in a specific geographic area. Directory queries may be directed to the Active Directory through the Active Directory Service Interface (ADSI), Lightweight Directory Access Protocol (LDAP), and standard Microsoft networking (a modified form of the Universal Naming Convention (UNC)).

2.2 Security

Windows® 2000 includes a diverse set of standard security features that are available programmatically through the Security Support Provider Interface (SSPI). A major security component is the integrated Kerberos network authentication protocol providing strong authentication through applied secret-key cryptography. To complement standard user authentication, additional security services include: the Encrypting File System (EFS), Public-Key Infrastructure (PKI), Smart Card, Internet Protocol (IP) Security (IPSec), and Virtual Private Network (VPN).

2.2.1 Kerberos

The cornerstone of Windows® 2000 security is the implementation and use of Kerberos version 5 from the Massachusetts Institute of Technology. Kerberos is the default user authentication mechanism for Windows® 2000. Although the Windows® NT LanManager (NTLM) authentication mechanism is retained for downlevel compatibility, the Kerberos architecture, encryption scheme, and key management are greatly superior to NTLM. Kerberos keys are managed by the Kerberos Key Distribution Center (KDC), which is integrated with Windows® 2000 security services on the domain controller. The Active Directory is used for the storage of the security accounts database.

Microsoft has extended the Kerberos protocol to permit use of a public key for initial authentication versus conventional shared secret keys. This extension is used to support the use of Smart Cards for interactive logons. Interoperability with other Kerberos implementations continues to be an active area of investigation.

2.2.2 Encrypting File System (EFS)

Windows® 2000 is the first version of Microsoft's advanced operating systems to natively support technologies providing easy insertion and removal of hardware (e.g., Plug n Play, Advanced Configuration and Power Interface). Along with the introduction of support for notebook computers and Plug n Play devices such as removable hard disks, Windows® 2000 provides a media encryption/decryption capability, the Encrypting File System. The EFS requires the media to be formatted as a version 5 NT File System, NTFS v5. EFS encryption/decryption services are embedded in the Windows® 2000 kernel, and may be configured to encrypt/decrypt an entire drive, or selected directories or files. EFS is not available on floppy disks due to the overhead of NTFS and NTFSv5, versus the older File Allocation System (FAT, FAT16, FAT32).

The Windows® 2000 kernel automatically detects encrypted files during file input/output. A user's certificate and associated private key are located in the user's certificate within the Active Directory, and file encryption and decryption are accomplished automatically and transparently.

System "Data Recovery Agents" may be configured to use a file's randomly generated encryption key to recover an encrypted file, directory, or drive. A Windows® 2000 domain recovery policy may also be configured, delegating the role and responsibility of data recovery to a select group of users within a domain.

2.2.3 Public Key Infrastructure (PKI)

Although a set of PKI services became available in Windows® NT 4.0, Windows® 2000 integrates an enhanced set of PKI capabilities to complement the standard authentication and trusts services provided by Kerberos. The PKI services enhance the native Windows® 2000 security services to better address intranet and extranet needs, including: scalability and distributed identification, user authentication, data integrity, and confidentiality. Further, the Windows® 2000 PKI assumes a hierarchical Certificate Authorities (CA) model for purposes of

scalability and support for third-party products (e.g., VeriSign, Thawte). This includes several components: (1) Windows® 2000 Certificate Services using ITU-T X.509 v3-based certificates, (2) integration of CAs issuance and revocation with the Active Directory, and (3) use of standard PKCS-10 certificate request messages and PKCS-7 responses. The initial certificate offering supports three encryption key/signatures: Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and Diffie-Hellman.

2.2.4 Smart Cards

Smart cards may be optionally used for Windows® 2000 logon. Use of Smart Cards is controlled via user account information in the Active Directory. Smart Cards are also a convenient mechanism for storing user keys (e.g., private keys, encryption keys), and user's certificates (issued by an enterprise CA).

2.3 Network

Another area in which Windows® 2000 is more than "just another Windows® NT", is the new and enhanced network services. From the new default network protocol of TCP/IP, to the optional network packet encryption, to quality of service and bandwidth allocation and management, to IEEE 802.1p prioritized local area networks (LANs), virtual private networks, and multicast protocols, Windows® 2000 networking has significantly changed. The Active Directory is used to specify users' access rights and for the storage of keys.

2.3.1 TCP/IP

Traditionally the preferred and default network protocol for the Windows® family of operating systems has been the NetBEUI (NetBIOS Extended User Interface) protocol, a non-routable protocol. Windows® 2000's preferred, and default, network protocol is the industry standard TCP/IP suite of network protocols. Installation wizards ease the installation process, and assume the presence of a DHCP server to ease address assignment, although DHCP is not required.

This is the first release of any Windows® OS to natively support the suite of industry standard multicast protocols used on the Multicast Internet (MBONE) for services like collaboration. Additionally, new network interfaces are supported including Asynchronous Transfer Mode (ATM) and prioritization of LAN traffic via the IEEE 802.1p standard.

2.3.2 IP Security Protocol (IPSec)

The Internet Protocol Security Protocol (IP Sec) is a set of protocols being developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets, network-level authentication, data integrity, and encryption. Windows® 2000 implements this service below the transport level. IPSec keys and associated key management is integrated in the Active Directory, enabling central control of policy-based security administration. IPSec is also used in the Windows® 2000 implementation of Virtual Private Networks (VPNs).

Windows® 2000 makes full use of industry-standard cryptographic algorithms and authentication techniques to include:

- Diffie-Hellman technique to agree upon a shared key.
- Hash message authentication code (HMAC) and variations, to provide integrity and anti-replay.

There are a number of industry efforts to define and implement key management. Currently Windows® 2000 supports the following conventions:

- Internet Security Association and Key Management Protocol
- Oakley Key Determination
- IP Authentication Header
- IP Encapsulating Security Protocol

2.3.3 Quality of Service (QoS)

There is a category of applications that use data that is isochronous and bursty in nature. A good example is collaboration where voice and video (camera) streams are commonplace. Both voice and video data demonstrate these characteristics. Quality of service is the ability to define, request, allocate, and manage a number of network services including network bandwidth and error rate thresholds. Microsoft has defined a set of Windows® 32-bit APIs (Win32) supporting these services. Realization of an end-to-end QoS capability necessitates that all components between the sending and receiving computers provide support for these QoS parameters. One of the protocols within Windows® 2000 that supports QoS is the resource ReSerVation Protocol (RSVP).

2.3.4 Virtual Private Network (VPN)

Use of the Internet to interconnect geographically dispersed office locations is an example of IT "outsourcing." Unlike the dedicated end-to-end circuits where an organization "owned" and managed the links, use of open resources like the Internet raises security concerns. Virtual private networks are the set of technologies and techniques to tunnel network traffic between sites. When VPN is used, all network traffic between sites is encrypted using any number of standard algorithms.

Windows® 2000 supports VPNs using an improved Point-to-Point Tunneling Protocol (PPTP) and Level 2 Tunneling Protocol (L2TP), as well as user authentication and data encryption using L2TP with IPSec. As with any key-based technology, key management is critical. In Windows® 2000, the Active Directory is the repository for all keys.

2.4 Management

Windows® 2000 provides a more complete and unified set of management APIs and services than Windows® NT. In addition to the Windows® NT Windows Management Instrumentation (WMI) approach, Windows® 2000 augments these management capabilities to include Active

Directory and the Microsoft Management Console (MMC). The MMC became available for Windows® NT, and has become an integral part of Windows® 2000 for management of all related services.

2.4.1 IntelliMirror

IntelliMirror is a set of change and configuration management capabilities designed to assist in centrally automating administration and management of software installation, repairs, updates, and removal; remote installation of the operating system; and mirroring of user data to the network and to local copies of selected network data. These capabilities are controlled through Windows® 2000 policy-based management. A major use of this technology is support for users who travel from one office or site to another as part of their operational responsibilities (e.g., roaming users). There are four basic areas:

- Software Installation allows a user's software to follow users from one machine to another.
- Remote Operating System Installation provides administrators the ability to remotely install the Windows® 2000 OS in a manner similar to Sun Microsystems' "JumpStart" capability.
- User Data Management ensures a user's data and documents follow the user.
- User Preferences/Settings enable user-specific software "customizations" or preferences to follow users as they travel.

2.4.2 Windows® File Protection

It has always been a challenge to manage dynamic link libraries (DLLs). On occasions a vendor's software would require some unique services or feature, which is included in an "updated" DLL. All too often this "updated" DLL replaces another DLL and introduces anomalies. Windows® 2000 provides a monitoring and change control mechanism, the Windows® File Protection (WFP), a process (i.e., daemon) that monitors select files in specific locations and prevents the replacement of essential system files. Currently WFP monitors two directories **%SystemRoot%** and **%SystemRoot%\system32** for writes to ***.SYS, *.DLL, *.EXE, and *.OCX** files. If WFP detects such activity, the original file is copied from **%SystemRoot%\system32\dllcache**. In cases where multiple DLLs of the same name are required, the Microsoft Application Specification for Microsoft Windows® 2000 for desktop applications recommends placing vendor-specific files in **%ProgramFiles%\<company name>\<App Name>**, or **%ProgramFiles%\<company name>\Shared Files**.

2.5 Scalability / Robustness

Windows® 2000 Advanced Server and DataCenter Server includes the full feature set of Windows® 2000 Server and adds the high availability and scalability required for enterprise and large departmental solutions. Key scalability and robustness features include Network Load Balancing and the Microsoft Cluster Service. Scaling up the processing power through symmetric multiprocessing (SMP) and increased memory addressing is also supported in Professional and all versions of the Windows® 2000 Server.

2.5.1 Clustering

In the Windows® 2000 Advanced Server and DataCenter Server operating systems, Microsoft introduces two clustering technologies, Network Load Balancing (NLB) and Cluster Services, which can be used independently or in combination. A third service, Component Load Balancing, will be available at a later time as part of a future product, AppCenter Server.

Network Load Balancing

Network Load Balancing (NLB) provides scalability and high availability of TCP/IP-based applications and services by combining up to 32 servers running Windows® 2000 Advanced Server into a single, load balancing cluster. The NLB server distributes IP requests to the most available server in the cluster. It provides failover and the ability to swap servers in and out without interrupting service. The most likely use for NLB is for a Web server farm wherein NLB distributes incoming Web requests among its cluster of IIS applications.

Network Load Balancing is designed to work as a standard networking device driver. TCP/IP must be installed in order to take advantage of NLB functionality. With NLB, the cluster appears as a single IP address from the outside. The current version of NLB operates on Fiber Distributed Data Interface (FDDI) or Ethernet-based local area networks within the cluster.

Cluster Services

Cluster service lets you combine two servers to work together as a server cluster to ensure that mission-critical applications and resources remain available to clients. If one server in the cluster fails, another server will automatically take over. There is an instance of the Cluster Service running on every node in a cluster. Specifically, the Cluster service manages cluster objects, cluster disks, and their configuration, handles event notification and performs failover operations. Windows® 2000 Advanced Server supports two-node clusters and DataCenter Server supports four-node clusters.

Before an application can use cluster failover, the following are required:

- Client and server applications must use TCP/IP (or Distributed Component Object Model, Named Pipes, or Remote Procedure Call over TCP/IP) for their network communications.
- The disks must be attached to a shared disk bus.
- The application must reside on all nodes in the cluster.
- Upon failure, the application must be designed to be restarted automatically.

During failover, client applications experience a temporary loss of service availability. If you configure the client application to recover from temporary network connection problems, it can continue operating after a server failover.

Applications that keep significant state information in RAM are not the best applications for clustering because information not stored on disk is lost at failover. Applications that use the

Cluster API can register with the Cluster Service to receive status and notification information, and the applications can use the Cluster API to administer clusters.

NLB and Cluster Services can be used together on the same network but not on the same server. Nodes in a server cluster can be member servers or domain controllers. However, in either case, both nodes must belong to the same domain. A typical configuration for a web application is to use NLB to distribute the load to a group of web servers that share a single IP address. Within this application Cluster Service might be used in the backend for file services, messaging, and databases that support the web servers.

Component Load Balancing

Component Load Balancing (CLB) for middle tier COM+ applications servers was provided in some of the earlier releases candidates for Windows® 2000. The intent of CLB is to distribute workload across multiple servers running a site's COM+ business logic, which is a more scalable version of the Microsoft Transaction Server (MTS) technology available through Windows® NT 4 Server using Option Pack 4. CLB complements both NLB and Cluster Service by acting on the middle-tier of a multi-tiered clustered network. Microsoft recently announced the elimination of CLB from Advanced Server and DataCenter Server and the redeployment of the capability to the upcoming AppCenter Server. This change was effective with Windows® 2000 Release Candidate 2 (RC2).

If a Web-based application were developed without CLB, you might choose to deploy COM+ on the same physical IIS servers. By doing this, the application servers can take advantage of the scalability and availability gains afforded by the existing NLB cluster without any need for an additional, separate tier of dedicated servers running COM+, which could help reduce hardware and management costs.

2.5.2 Symmetric Multi Processing (SMP)

Symmetric Multi Processing enables any one of the multiple central processing units in a computer to run any operating system or application thread simultaneously with other processors in the system. Windows® 2000 Server will provide up to four-way SMP. Advanced Server will support up to eight-way SMP and DataCenter Server supports up to 32-way SMP. Windows® 2000 Professional provides up to two-way SMP support. In conjunction with SMP, Advanced Server can address 8 GB of memory and DataCenter Server will be able to address 64 GB. Significant scalability beyond that possible with Windows® NT Server is possible when you consider the 4-to-32 processors SMP, the larger address ranges, and the clustering options.

2.5.3 Terminal Server

Terminal Server is an integral component of Windows® 2000 servers, extending the native Windows® interface (i.e., screen, keyboard, mouse) across the network to machines that normally would not be able to run Windows® applications. This capability is similar to the X Window model used in UNIX environments. Remote users have complete Windows® 2000

functionality to run native Microsoft Windows® applications including the Active Directory and the full suite of systems administration and management applications. The Remote Desktop Protocol (RDP) is the communications protocol between the Terminal Server and its clients, necessitating installing a Terminal Server Client driver on each client workstation. Microsoft provides clients for the Windows® family of OSs. Client support for non-Windows® is expected to become available from third-party companies like Citrix and NCD, both of which have add-ons for the optional Windows® NT-based Terminal Server.

Licenses for Terminal Server are separate from the Windows® 2000 Server and are related to the Terminal Services Client.

3. ADOPTION / DEPLOYMENT CONSIDERATIONS

There are several motivations for this section. The new and enhanced services and features of Windows® 2000 coupled with the possibilities of receiving no-cost upgrades from Windows® NT may be so enticing that some users might install Windows® 2000 before the IT organizations have a well-defined set of guidelines.

There are several items to consider:

- Windows® 2000 is not another version of Windows® NT
- Microsoft has spent in excess of four years teamed with partners developing, integrating, and testing this new suite of technologies
- Between July 1993 and July 1996 Microsoft released four versions of Windows® NT: v3.1, v3.5, v3.51, v4.0
- The most crucial component is a new enterprise-level directory service.

These considerations alone should caution information technology (IT) professionals. When you consider that these four plus years addressed few DOD-unique heterogeneous concerns, it would be prudent for IT organizations to formulate a deployment plan based on needs.

The following sections categorize considerations that an IT organization should address to manage and monitor the introduction of a major release of Microsoft's Windows® 2000 operating systems.

3.1 Preparation – "Plan Twice, Deploy Once"

Microsoft has designed Windows® 2000 to appear as the next Windows® NT offering, to offer many attractive features, and to interoperate with their Windows® family of operating systems. However, there are significant enhancements included in Windows® 2000, and these enhancements have yet to be "field tested" in a model of a real-world operational DOD environment. As IT professionals, it is important to avoid unnecessary interruptions of service as we provide a quality, reliable infrastructure.

The key message from this investigation of new and promising technologies is that DOD IT organizations should avoid introducing these technologies without careful planning and

experimentation. Although Windows® 2000 has many new and attractive features, DOD IT organizations should first test Windows® 2000 in a controlled environment where performance and other metrics can be monitored and measured, while planning a systematic introduction of Windows® 2000.

3.2 Directory Services

The new integrated directory service provides the crucial link for all Windows® 2000 offerings: one source for name resolution, whether it be a machine name, or location of domain servers, of a Component Object Model (COM) object, of Java classes, or of a printer. Most organizations that were beta testers of Windows® 2000, members of early deployment teams, and technical reviewers stress the importance of designing the Active Directory and Network Design carefully. To reinforce these practices, Microsoft's Deployment Planning Guide[2] has two major sections: "Active Directory Infrastructure" and "Network Infrastructure Prerequisites."

The number of interfaces and protocols supported by the Active Directory should be an indication of the magnitude of name resolution integration. IT roll-out of the Active Directory presumes a good understanding of enterprise directory services like dynamic DNS, X.500 directory structure, LDAP, certificates, encryption keys, quality of service parameters, and Email addressing. Additional IT considerations include: Windows® 2000 transitive domain trusts; the use of directory space "partitions"; synchronization among the many Active Directory replicas on an enterprise's Windows® 2000 domain controllers; synchronization impact on the network; and Active Directory's ability to synchronize with existing directory services like DMS, Netscape Directory Server, and Sun's Directory Server.

3.3 Network (Distributed) Services

It is difficult to clearly identify a technology as strictly "the network"; it is more accurate to define a network as the set of services that are made available via the network. In Windows® 2000, the most important and crucial network service is the Active Directory, the central repository for Windows® name resolution. However, the inclusion of new network protocols like dynamic DNS, RSVP and Multicast Internet (MBONE), security mechanisms like VPN and IPSec, and network quality of service (QoS), system stability, integration, interoperability, and impact on legacy systems needs to be resolved. Management of electronic keys for technologies like Smart Cards, VPNs, and IPSec is also an issue.

3.4 Application "Breakage" & Locked Folders

When an operating system vendor releases a new version, there is always concern about backward compatibility—will the applications that ran on the currently installed version run with the new OS? Initial testing has indicated that the majority of Windows® NT 4.0 applications which use the 32-bit API set (Win32) and followed good design and implementation guidelines,

---

[2] (http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp)

are expected to work with Windows® 2000. Application incompatibilities are expected in two areas: application installation, and new Windows® 2000 protection features.

One of the most popular reasons an application does not install is incorrect handling of operating system and dynamic link library (DLL) version numbers. The installation scripts incorrectly check the major and minor version numbers. For instance, if the version of the OS is not 3, and the OS version is not 4, then the script cannot install and the script terminates. In many cases application installation scripts assume that dependent components exist based on OS version number.

Several new protection features have been incorporated into Windows® 2000. The most important is the "locking down" of select system directories: **%SystemRoot%** and **%SystemRoot%\system32**. In prior versions of Windows®, vendors would place files in these directories without warning the user of filename and file version conflicts that contributed to system instability. Application installation scripts which expect to use either of these directories will not install. Another feature of Windows® 2000 is the ability to have multiple versions of files installed and running "side-by-side". The new guidelines state that all vendor-specific code must be installed in either the **%ProgramFiles%\<company name>\<App Name>** or in **%ProgramFiles%\<company name>\Shared Files** directories.

Many installation scripts assume that the **%SystemRoot% and %SystemRoot%\system32** directories are available for (or should be used for) installing vendor-specific software. Since Windows® 2000 locks these folders, except for Microsoft code, this will "break" some installation scripts, necessitating revising installation guidelines.

3.5 Information Security

Windows® 2000, like Windows® NT, is a tightly integrated system of many modules and services. It is unclear what Windows® 2000 services are bundled into the standard installation of the OS, how to "remove" unnecessary services, service dependencies, and what impact components might have on system operation. With the inclusion of Active Directory and an enhanced version of Kerberos v5, some of the concerns include:

- The transitive two-way trusts between domains may impact your Windows® NT domain architecture, user authentication, and administration.
- Access control can now be specified with finer granularity in the Active Directory.
- Additional Kerberos features may introduce interoperability issues.
- The integrated PKI, certificates, and encryption algorithms may not interoperate with the DOD PKI.
- Interoperation between multiple implementations of IPSec and VPNs has not been assessed.
- Upgrading to Version 5 of the NTFS and the optional Encrypting File System (EFS).
- Electronic key management within Windows® 2000 and with heterogeneous systems needs clarification.

3.6 Bundling / Licensing

Microsoft has four configurations (versions) of Windows® 2000, ranging from the desktop workstation (Windows® 2000 Professional), to three levels of servers: Server, Advanced Server, and Data Center. The basic capability is configured in Professional with increasing capability through the line of server products, with the complete set of Windows® 2000 functionality available in the DataCenter version. See Table 1 for additional information.

Microsoft has a number of licensing alternatives for commercial programs including special programs for large enterprises like the DOD. Some of these DOD licensing and procurement vehicles provide for FREE upgrades of the operating system for recently purchased computer systems. If the only FREE upgrade is for the desktop Professional version, and an enterprise has a Windows® NT environment, there should be minimal, if any, interruptions in operations. However, the unplanned introduction of any server version which installs the Active Directory will significantly raises the probability of introducing interruption of operational services. To help mitigate any interruption of enterprise service, IT organizations need to have and publish a plan for upgrading and installing Windows® 2000 server and the Active Directory.

3.7 Hardware "Footprint"

With each release of Microsoft's "flagship" operating system, Windows® NT, the stated minimum hardware requirements were sufficient for the operating system, but did not include any "typical" suite of software applications. The stated minimum Windows® 2000 requirements in Table 1 do not reflect the needs of application software. Thus, for planning purposes, the minimum suggested system footprints are:

	Compatible Central Processing Unit	Speed Mega Hertz (MHz)	Random Access Memory (RAM)—Mega Bytes (MB)	Available Hard Disk Space—Giga Bytes (GB)
Professional	Pentium II	200	128	2
Server	Pentium II	200	128	4
Advanced Server	Pentium II	300	256	8

Table 2: Minimum Suggested Hardware Footprint

In preparation of installing Windows® 2000, there is a free Microsoft utility, the Windows® 2000 Readiness Analyzer, which when executed in a Windows® environment, will examine the hardware and software configuration of a PC, and report discovered configuration abnormalities. Based on this report, IT organizations should be better prepared to assess the viability of using existing systems for Windows® 2000 systems. Some typical discoveries include a machine's basic input/output system (BIOS) support for plug-n-play, and power management (e.g., Advanced Configuration and Power Interface). This utility also identifies software components that will need to be replaced like device drivers (e.g., network interface cards—NIC, mouse, joystick, sound, video card).

3.8 Administrative Services

There are many aspects of management in Windows® 2000. To provide a consistent, unified interface, Microsoft introduced, in Option Pack 4 for Windows® NT 4.0, a new standard interface for management, their Microsoft Management Console (MMC). MMC is the standard interface for Windows® 2000 management.

There are multiple dimensions of management, including: users and machine accounts, support for the roaming users, software distribution and installation, granularity of administration delegation, allocation and management of network bandwidth/services, and the enterprise directory and its services. Considering the diversity of management capabilities and the mechanisms to support an infrastructure, it is important for the IT organization to define a Windows® 2000 management plan including which groups (of people) will have the roles and responsibilities to establish and maintain such a plan. This plan will need to address:

- Active Directory synchronization within an organization, and with heterogeneous directory services
- IntelliMirror's support for roaming users and the distribution and installation of software
- Extending the Active Directory's schema to support unique enterprise needs
- Fine-grain allocation and delegation of management of Active Directory objects
- Remote installation of software
- Requesting, allocating, and managing network quality of service
- Support for mixed environments: Windows® NT 4.0 and Windows® 2000; Windows® and non-Windows® (e.g., UNIX)

Given the number of additional technologies in Windows® 2000 such as dynamic domain name service (DDNS), X.500-based directory service, network protocols (e.g., multicast, IP Security), and security (e.g., public key infrastructure), it is paramount that IT organizations plan to train their technical engineers and support staff to better understand the features and tradeoffs of Windows® 2000 before introducing Windows® 2000 into an operational environment. It is preferred that an IT organization, **"Plan Twice, Deploy Once"**.

3.9 Software Distribution & Compatibility

An integral component of Windows® 2000 is the ability to use the Component Manager to define units of installable software known as components, with later "push" of this software component to one or more Windows® 2000 systems. This capability is also used to support an organization's roaming users. Automating the installation can assist an enterprise to deliver software and ensure their systems have a consistent set of software, but there are two considerations IT organizations need to address and plan for: network traffic/bandwidth consumed for a component "push", and impact on software licenses.

3.10Deployment

The decision to deploy Windows® 2000 in an operational environment requires careful consideration. The most significant consideration is the impact Windows® 2000 will introduce into your operational environment. The general consensus is that deployment will be lengthy primarily based on the need to properly design an architecture for the X.500-based Active Directory. For IT organizations having either legacy Windows® NT domains or X.500-based directory services, the additional issues of interoperability (coexistence) with legacy systems, or migration to the Active Directory require planning and resources.

If an IT organization has to support Windows® 2000, since Windows® 2000 Professional (workstation) can coexist in a Windows® NT domain environment, and the Professional version does not have an Active Directory, the Professional version could be used with minimum, if any, interruptions of service. However, Windows® 2000 is not Windows® NT 5.0; there are significant enhancements necessitating an IT organization's training.

In contrast to promotional material, there are no “Free Upgrades.” The preparation necessary to support Windows® 2000 includes: verification of interoperability with legacy systems—Windows® - and non-Windows® -based; training of personnel, verification that legacy applications continue to function properly; and verification that Windows® 2000-based systems do not interrupt (deny) normal operations and service. Industry consensus is not to deploy Windows® 2000 until there is additional knowledge and experience with Windows® 2000 in an operational, heterogeneous environment, preferably a prototype of a mission-critical environment.

For UNIX/Windows® 2000 heterogeneous environments, there is an optional Microsoft package “Windows Services for UNIX 2.0” containing many UNIX commands and environments including Network File System (NFS) Client, NFS Server, PCNFS Server, NFS Gateway, Korn shell, telnet client and server, ActiveState PERL, 60+ UNIX commands, Network Information System client and server, and password synchronization between UNIX NIS and the Active Directory. Other vendors provide similar sets of software.

4. CONCLUSION

Microsoft and its numerous partners have spent four plus years in preparing Windows® 2000 for commercial availability in February 2000. When you consider that most of these fours years were spent focused on a Windows®-centric perspective, an IT organization supporting a heterogeneous environment must ensure they are prepared to support a diverse set of capabilities in Windows® 2000, and that there are few guarantees of heterogeneous interoperability.

The newest version of Microsoft’s flagship operating system is more than just the next version of Windows® NT. It is substantially more than Windows® NT, to the point that an IT organization must understand how well Windows® 2000 will “fit into” their environment before installing the first occurrence of a Windows® 2000 domain server. Once an organization has installed an Active Directory, the resources necessary for any recovery are difficult to calculate.

IT organizations in which Windows® 95, Windows® 98, or Windows® NT are present should not ignore Windows® 2000. Rather those organizations need to develop and publish a plan and strategy for Windows® 2000 desktop and server versions. Many organizations that participated in Microsoft's Rapid Deployment Program have tested Windows® 2000 in a controlled lab. Figure 2 illustrates a sequence of activities an IT organization should consider before introducing Windows® 2000 Active Directory. When an IT organization reaches the "Decision" box, they should have sufficient information on deployment issues like robustness, stability, interoperability, disruption of IT services, and application breakage, to make an informed decision.

For IT organizations that are primarily Windows® NT-based, Windows® 2000 is very attractive and compelling, and has fewer risks in migration than a heterogeneous environment. However, if your organization is heterogeneous like the DOD, the Windows® 2000 features may not be as compelling, especially when you consider the mixture of operating systems and provided services.

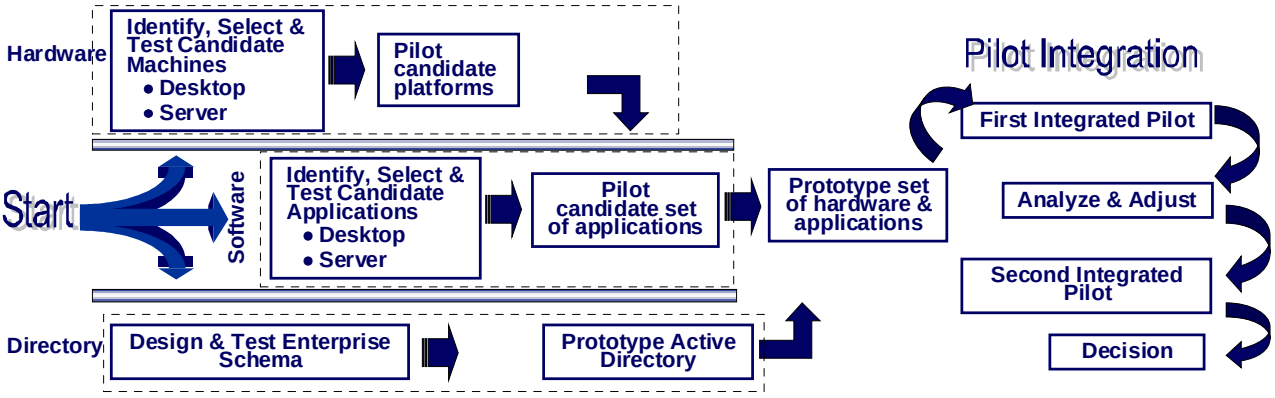

Figure 2. Steps Before Introducing Windows® 2000 Active Directory

In summary, any IT organization contemplating deploying Windows® 2000 should consider the following activities:

Don't Be An Early Adopter: Although Windows® 2000 has many new and useful capabilities, there is little testing of Windows® 2000 in an "real world" DOD environment. Windows® 2000 has been developed as the "one stop shopping" for name resolution (e.g., DNS, DHCP, LDAP). Since most operational environments contain one or more of these services, the introduction of the Active Directory (Windows® 2000 domain controller) into an operational environment may result in degraded services and possibly complete short-term disruption of services. To reduce such catastrophic scenarios, it is recommended that an IT organization first test Windows® 2000 in a near "real world" environment.

Be An Early Tester: If an IT organization has a Windows® NT environment or is considering introducing Windows® 2000-based software into their organization, the first IT organization activity should be the definition of a well thought out plan for assessing the "readiness" of their environment, to include: desktop and server hardware, network

infrastructure, selection of network protocols and services, selection of application software, integration with legacy systems, and overall enterprise system performance. The IT organization should then follow this plan, making key decision along the way whether Windows® 2000 is ready for their organization, or further assessment is necessary. Use of prototypical systems is key for an IT organization to more accurately assess impacts of Windows® 2000-based systems and software within an operational environment.

Develop Guidelines: This plan is similar to the testing plan identified above, it enumerates when and how Windows® 2000 is officially introduced into and supported in an operational environment. Based on the results and "lesson learned" from the early testing, an IT organization will need to accomplish several activities before allowing full deployment of Windows® 2000. These activities include: design of the enterprise's directory services—Active Directory, Windows® domain structures, defining administrative activities and permissions, training support personnel including the help desk, software development policies if appropriate, and migration strategy.

In all cases, if a Windows® environment exists or is contemplated, IT organizations need to prepare:

Plan Twice, Deploy Once

LIST OF REFERENCES

In the preparation of this document, many white papers, briefings, web pages, and other forms of information were used to assimilate a "view" of Microsoft's new product, Windows 2000.

White Papers

"Is Microsoft's NT/Windows 2000 Enterprise-Ready", January 2000, Aberdeen Group

"Active Directory Technical Summary", 1999, Microsoft

"NT TCO and Migration", 1999, Gartner Group

"Windows 2000", 1999, Gartner Group

"NT Scenario", 1999, Gartner Group

"Windows 2000: Start Thinking About Microsoft's New Operating System", 1999, TechRepublic

Web Site (URLs)

Aberdeen Group

http://www.aberdeen.com/middleeast/gitex%5Fwin2000/sld001.htm
"The Arrival of Windows 2000: Technology and Deployment"

ComputerWorld

http://www.computerworld.com/home/news.nsf/all/9910181win2k
"Tech Analysis: Win 2K -- Forget NT, this is something very different"
http://www.computerworld.com/home/news.nsf/all/9909094ggw2kcost
"Gartner predicts high Win 2K costs"

ent Online Magazine

http://www.entmag.com/displayarticle.asp?ID=1299932505PM
"Early Adoption and Windows 2000"

Microsoft

http://www.microsoft.com/Windows2000/default.asp
"Application Specification for Microsoft® Windows® 2000 for Desktop Applications"
"Server Specification for Microsoft® Windows® 2000 for Desktop Applications"
"Planning Migration from Windows NT to Windows 2000"
http://www.microsoft.com/windows2000/library/planning/default.asp
http://www.microsoft.com/windows2000/en/professional/help/default.asp
http://windows.microsoft.com/windows2000/en/server/help/default.asp
http://windows.microsoft.com/windows2000/en/advanced/help/default.asp

http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp

"Deployment Planning Guide", very good guide covering diverse deployment (migration) considerations and step-by-step procedures

http://msdn.microsoft.com/certification/default.asp

"Certified for Windows Program"

TechWeb

http://www.techweb.com/se/directlink.cgi?INW19990712S0002

"Directory Powered: Enterprise Play: MS Buys Zoomit"

http://www.techweb.com/wire/story/TWB20000125S0006

"HP, Compaq Outline Windows 2000 Strategies"

Windows NT Magazine

http://www.WinNTMag.com/

"What Microsoft Hasn't Told You About Deploying Win2K"

"Migrating to Windows 2000"

LIST OF ACRONYMS

AD	Active Directory
ACPI	Advanced Configuration and Power Interface
ADSI	Active Directory Service Interface
ATM	Asynchronous Transfer Mode
BIOS	Basic Input/Output System
CA	Certificate Authority
CALS	Client Access Licenses
CLB	Component Load Balancing
COM	Component Object Model
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
DC	Domain Controller
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DMS	Defense Messaging System
DNS	Domain Name Service (non-dynamic)
DSA	Digital Signature Algorithm
EFS	Encrypting File System
FAT, FAT16, FAT32	File Allocation Table, File Allocation Table 16-bit, File Allocation Table 32-bit
FDDI	Fiber Distributed Data Interface
GB	GigaByte

GC	Global Catalog
HMAC	Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILS	Information Locator Service
IP	Internet Protocol
IPSec	IP Security
IT	Information Technology
ITU	International Telecommunication Union
KDC	Key Distribution Center
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MB	MegaByte
MBONE	Multicast Internet
MMC	Microsoft Management Console
MTS	Microsoft Transaction Server
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input / Output System
NFS	Network File System
NIC	Network Interface Card
NIS	Network Information System
NLB	Network Load Balancing

NT	New Technology
NTFS	NT File System
NTLM	NT LanManager
OS	Operating System
PC	Personal Computer
PCNFS	PC Network File System
PERL	Practical Extraction and Reporting Language
PKCS	Public-Key Cryptography System
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RAM	Random Access Memory
RAS	Remote Access Service
RC2	Release Candidate 2
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman
RSVP	resource ReSerVation Protocol
SMP	Symmetrical Multi-Processor
SSPI	Security Support Provider Interface
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
UNC	Universal Naming Convention
VPN	Virtual Private Network

WAN	Wide Area Network
WFP	Windows File Protection
WINS	Windows Internet Name Service
WMI	Windows Management Instrumentation